Crisis Warning Apps: Investigating the Factors Influencing Usage and Compliance with Recommendations for Action

Diana Fischer
University of Bamberg
diana.fischer@uni-bamberg.de

Johannes Putzke-Hattori
University of Bamberg
johannes.putzke-hattori@uni-bamberg.de

Kai Fischbach
University of Bamberg
kai.fischbach@uni-bamberg.de

Abstract

Effectively disseminating warnings of threats such as floods, thunderstorms, or terrorist attacks is essential for saving lives in affected areas. With the widespread use of mobile devices such as smartphones, mobile warning applications (warning apps) enable the efficient transmission of warnings via push-notifications. Use of warning apps in crisis or threat situations, however, has received little attention by researchers. Therefore, we investigate in this study the factors that affect the use of warning apps and the intention to comply with recommendations for action transmitted via such apps. We rely on prior research that studied compliance intention during campus emergencies, research on warning and risk communication, and research on technology usage. We find that risk perception, trust, and subjective norm positively influence both use of a warning app and compliance intention, whereas concerns about data security have negative effects. Our findings inform research in the context of risk communication and technology usage as well as providers of warning apps seeking to promote their apps effectively.

1. Introduction

The worldwide trend in recent years has been for larger, more frequent, and costlier crisis events due to climate change, deforestation, urbanization, global inequality, and political instability [28, 43]. Examples of such large-scale events range from human-made crises such as the 9/11 terrorist attacks in 2001 to natural crises such as Hurricane Katrina in 2005 and earthquakes such as Haiti's in 2011, and to the combination of earthquake, tsunami, and nuclear meltdown in Fukushima that same year. These sorts of large-scale crises have enormous consequences for the affected population. So, too, do small-scale crises that receive far less media attention: a flash flood that damages only a few houses can still have severe consequences for individuals and a community [43].

Effective, timely warnings should reach all people at risk no matter what they are doing or where they are located. They are key to protecting the population from the potential consequences of both large and smaller, more localized crisis events. As smartphones have become an integral part of everyday life and are increasingly used worldwide [35], they have great potential for transmitting warning messages. In particular, mobile warning applications (hereafter called warning apps) that run on mobile devices such as smartphones can help disseminate warning messages effectively.

Unlike other information and communication technologies (ICTs) such as social media, such apps are used only for communication from authorities such as the U.S. Federal Emergency Management Agency (FEMA) and thus the user can easily trace the source of the warning, which is an important factor when an individual decides whether to trust a warning message [16]. Another advantage of these apps is that they warn users about a crisis via push-notification, requiring no action on the user's part [32]. Smartphone apps are, therefore, a fast, efficient, and far-reaching means of communication during crises.

While prior information security research has provided insights into factors driving the usage of campus emergency notification systems and compliance behavior during campus emergencies (e.g., [1, 2, 19, 20]), the current body of research has not addressed the factors influencing the use of warning apps in communities, nor has it accounted for the intention to comply with crisis warnings issued via such apps. To address this gap, this study addresses the following research questions: What factors drive the intention to use a warning app? What are the important factors that influence compliance intentions with crisis warnings via a warning app?

The paper proceeds as follows. The next section provides the theoretical background on warnings, mobile warning apps, technology usage, and our research model. Thereafter, we explain our hypothesis development. We then provide details on data collection, our methodology, and the results of our analysis. Finally, we discuss our results, the limitations

URI: https://hdl.handle.net/10125/59504
ISBN: 978-0-9981331-2-6

of our study, and future research directions, and we offer our conclusion.

2. Theoretical background

2.1. Mobile warning apps

A warning is a safety communication aimed at informing people about threats in their environment and persuading them to engage in protective behavior (i.e., comply with the warning) that would allow them to avoid or, at least, minimize undesirable consequences [45].

There are different ways to disseminate safety communications [8]; warnings about crises or severe weather warnings about floods, storms, and so on are distributed primarily via mass media such as TV or radio. However, those mass media are imprecise in that they also reach people who are at no risk and limited in that they only reach people who may be watching or listening, which logically excludes some of those affected [31]. In contrast, warning apps running on mobile devices such as smartphones enable precise and immediate distribution of warnings. In addition, warning apps transmit warnings via push-notification and thus people do not have to use the warning system actively; rather, they simply need to have their smartphones with them.

Generally, apps are self-contained software applications that can be downloaded to and run on smartphones. They are ways to receive information, access internet-based content, and watch and listen to video and audio media through an intuitive user interface [15]. Crisis communication research and practice has recognized the trend towards increased app and smartphone use in recent years and thus several mobile warning apps have been developed [15, 36].

As [36] state, mobile crisis warning apps must meet certain requirements to make effective contributions to disaster communication: ideally, they should be able to send warning messages, recommendations for actions, and all-clear messages; organize helpers; allow personal settings; show crisis-relevant emergency contacts; and contain a chat-function.

The FEMA, NINA, and KATWARN apps are all examples of warning apps [36]. Although they differ in some features, they share a core property: they serve to warn the population about potential dangers and supplement those warnings with recommendations for action. Recommendations for actions might be, for instance, to shelter in place in the case of a terrorist attack or not to drive into areas where water covers the roadway and move to higher ground immediately during a flash flood.

Apps have several advantages for crisis notification as compared to disseminating warnings via other ICT such as Facebook [13]. The user can easily trace the source of the message, which is an important factor when an individual decides whether to trust a crisis message [16]. In the case of the FEMA app, the source is obviously FEMA. Providers such as FEMA are considered legitimate sources for crisis warnings. Moreover, these apps can be used to transfer information to affected areas quickly via push-notification. An internet connection through a mobile data network and the availability of positioning services based on GPS via a smartphone allow for location-specific warnings at any time to a specific user. In addition to the localization of a smartphone, it is possible to select a region of interest that allows for receiving warning information specific to that region [32].

2.2. Warning systems and technology usage

While prior Information Systems (IS) research about crisis warnings has focused mostly on compliance intention and the use of warning systems such as social media or campus emergency notification systems during campus emergencies (e.g., [2, 19, 20]), insights from that research provide a valuable foundation for the present study. In addition, in IS research, the technology acceptance model (TAM, [11]) which has been further developed by [41] into a unified model (UTAUT), has made a significant contribution to technology usage research [42]. Warning app usage intention and compliance intention are the core constructs of our research model. Hence, we built on findings from these two research areas to develop our research model.

UTAUT explains behavioral intention based on four constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. The latter is an antecedent of actual usage behavior. Since behavioral intentions correlate significantly with actual behavior [3], various studies in IS security (e.g., [4, 20, 25, 26]) have adopted behavioral intention as a predictor of actual behavior, as have we. Since we are not examining actual usage behavior, we did not incorporate facilitating conditions in our research model [41].

Performance expectancy draws heavily from perceived usefulness. In the warning app context, this means the app is useful if warning messages and recommendations for action are reliable and timely so that people are able to protect themselves from danger. This explanation is also backed by prior research. For instance, [2] found that reliable and timely information via a crisis notification system is, in particular, a constant predictor of students' intention to use a campus notification system in various crises. Also, [20] identify

that trustworthy information transmitted via warning systems is a significant predictor of students' compliance intention in different campus crisis settings.

In addition, for a warning app to be perceived as useful, people have to perceive the risk of a crisis event in their environment about which they need to be warned [20]. Thus, we incorporate *perceived risk* and *trust* regarding the reliability and timeliness of a warning message as a predictor for usage intention and intention to follow recommendations for actions.

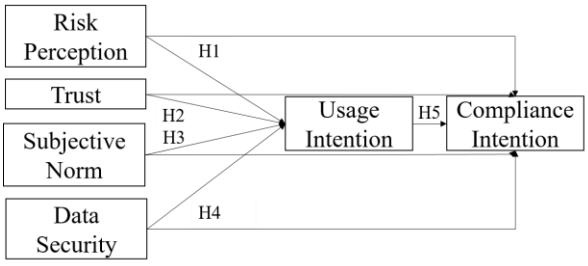
Social influence is a predictor for technology usage intention in UTAUT and also in line with previous research by [29] on college students' adoption of mobile-based text alerts via SMS (Short Message Service), [20] which indicates that *subjective norm* is a critical factor in students' compliance intention. [29] argue that warning systems are a socially driven technology and that even reluctant students can be significantly motivated to adopt such services by their important others.

Finally, effort-oriented factors are expected to be more influential in the early stage of a new behavior, when barriers must be overcome or when there is little experience with a system [41]. As a warning app is particularly easy to use for a regular smartphone user (the user only needs to download the app and decide on localization settings; warnings appear via push-notification), effort expectancy, which relies mainly on perceived ease of use, is less relevant to our research. However, when it comes to apps with localization settings, *data security* is an important and sensitive issue, which can negatively affect the use of that app [47].

Consequently, arguing that perceived risk, trust, subjective norm, and data security are important indicators for people's usage intention of warning apps, we incorporate these determinants into our research model. Our dependent variables are warning app usage intention, which indicates whether a person intends to use the app, and compliance intention, which indicates whether a person intends to comply with the recommendations for actions transmitted via the warning app.

Figure 1 depicts our overall research model.

Figure 1. Research model



3. Hypothesis development

Risk perception is defined as how an individual expects to be exposed to a crisis. Generally, people tend to overrate the likelihood of rare, serious crises and underrate the probability of more common, but less serious, events [37]. When confronted with a threat in one's own environment, people apply several complex decision-making rules to the rating of risk. For instance, people often misperceive seriousness, likelihoods, or their own true risk [40]. Yet it is risk perception and not actual risk that determines how people respond to threats in their environment [17].

The higher those risk perceptions of a person are, the more likely that person will try to protect himself or herself from the risk [20]. For instance, a high perception of being affected by flooding increases the willingness to take preventive measures against flooding [9]. Hence, we contend that the perceived risk of being exposed to a crisis such as flash flooding, a hurricane, or terrorist attack has a positive effect on the intention to use a mobile warning app and to comply with situation-specific recommendations for action, leading to the following hypotheses:

Hypothesis 1a: Risk perception positively affects the intention to use a warning app.
Hypothesis 1b: Risk perception positively affects the intention to comply with situation-specific recommendations for action.

Perceived trust relates to the information content of the warnings and behavior recommendations. Evidence shows that levels of trust strongly influence whether people take crisis warnings seriously [38]. Perceived trust is regarded as a significant influencing factor with regard to human behavior in emergency situations. For example, students are more likely to use a notification system for emergencies on campus when confidence in those notifications is high [2].

In addition, people in highly complex and uncertain crisis situations seem to have an increased need for reliable, timely, and useful information to aid them in making quick decisions about how to act [20]. Hence, trust in the information communicated in the warning is also imperative so affected people follow the recommended behavior. Further, confidence in the information influences compliance with behavioral recommendations in emergency situations [19]. Therefore, we hypothesize the following:

Hypotheses 2a: Trust positively affects the intention to use a warning app.

Hypotheses 2b: Trust positively affects the intention to comply with situation-specific recommendations for action.

Subjective norm is based on normative beliefs, that is, the perceived behavioral expectations of relevant others such as family, friends, supervisors, and/or coworkers. Normative beliefs, together with an individual's motivation to comply with the expectations of relevant others, determine the subjective norm [3]. There is evidence that if people perceive that using a warning app is the behavior expected by their relevant others, they will be more likely to use a warning app [20]. Furthermore, researchers have found that subjective norm positively affects compliance intentions in a security-related context in organizations [22]. Hence, we hypothesize the following:

Hypothesis 3a: Subjective norm positively affects the intention to use a warning app.
Hypothesis 3b: Subjective norm positively affects the intention to comply with situation-specific recommendations for action.

Crisis warnings from a warning app depend on the user's location. Users must allow access to their location to receive location-based warnings, or at least they must select a region of interest. This is typically done either by entering a postal code within the warning app or by activating the smartphone's internal tracking services [32].

However, individual privacy is a sensitive issue when using location-based mobile apps [47]. Also, research and theoretical implications from risk communication and warning credibility argue that information about the source of the information and the credibility of the source are important factors in an individual's decision to comply with warning messages [46]. Thus, concern about the lack of protection of personal privacy (i.e., "data security") could have a negative affect on the use of a warning app and on compliance with crisis warnings transmitted via the app. Hence, we further hypothesize:

Hypothesis 4a: Data security negatively affects the intention to use a warning app.
Hypothesis 4b: Data security negatively affects the intention to comply with situation-specific recommendations for action.

Usage intention indicates whether someone intends to use a mobile warning app to receive information about a crisis or a threat. Choosing to use a warning app indicates a person's interest in receiving warning messages and recommendations for action. Thus, people who intend to use a warning app should be likely to follow recommendations for action provided via the app. Also, prior research shows a positive correlation between behavioral intention and actual behavior (e.g., [7, 30]. Thus, we hypothesize the following:

Hypothesis 5: The intention to use a warning app positively affects the compliance with situation-specific recommendations for action.

The next section presents our methodology and findings.

4. Research method

4.1. Survey instrument

To perform an empirical test of the relationships suggested by our research model, we adopted a survey methodology approach for data collection.

In our questionnaire, we provided information on the features of a warning. We explicitly defined the term "warning app" to ensure that respondents had a common understanding of the subject and could see a warning app's potential as a means for receiving warning messages and recommendations for action. Specifically, we explained the features and properties of warning apps and gave two examples of the most familiar ones developed in and for Germany: NINA [44] and KATWARN [27].

Furthermore, we developed the initial set of items by analyzing the relevant literature for existing scales. The survey consists of closed-ended questions. All items use a 7-point Likert scale ranging from "strongly disagree" to "strongly agree." Most of the measurement items for the principal constructs were adapted from existing measures to the context of this paper to enhance validity. The items were fully pretested with 51 college students. We collected comments regarding, among others, the clarity and structure of the items, and we measured the time needed to answer the entire questionnaire (which also included some other items related to another research project). On average, it took respondents about 12 minutes. Based on the feedback, we revised the questionnaire and modified several items, especially with respect to their wording.

Table 1 is an overview of our final items and the corresponding constructs.

Table 1. Overview of the constructs and items

Construct	Items	Source
Risk Perception	RP_1: It is likely that I will be affected by a crisis in the future.	[2, 7]

	RP_2: It is likely that a crisis could affect my safety in the future. RP_3: It is likely that a crisis could affect my security in the future.	
Trust	Tr_1: Using a warning app, I will be informed by this app only when facing a crisis. Tr_2: I think I receive only relevant information using a warning app. Tr_3: I do not think that I receive an excessive amount of information.	[2, 20]
Subjective Norm	SN_1: Most people who are important to me would support me using an app that warns me of disasters and gives me behavioral recommendations. SN_2: Most people who are important to me think I should use an app that warns me about disasters and gives me behavioral recommendations. SN_3: Most people who are important to me would agree with my intention to use an app that warns me of disasters and gives me behavioral recommendations.	[6]
Data Security	DS_1: I am worried that the provider of the warning app will collect too much information about me. DS_2: I am afraid that the provider of the warning app will use information about me for other purposes. DS_3: I am afraid that the provider of the warning app will pass on information about me to third parties.	[34]
Compli-ance Intention	CI_1: If I receive via the warning app a notification that gives me situation-specific behavior recommendations, I will probably follow them. CI_2: I am sure that I will follow situation-specific behavioral recommendations I receive with a disaster notification via a warning app.	[22]
Usage Intention	UI_1: I intend to use a warning app for crisis notifications and recommendations for action. UI_2: I plan to use a warning app for crisis notifications and recommendations for action. UI_3: I predict I will use a warning app for crisis notifications and recommendations for action.	[7, 33]

4.2. Data collection and participants

For the final study, we conducted in March to June 2017 an internet-based questionnaire study by posting the link to the questionnaire on social media websites and forums in Germany. Because the target population of our study is the general public, we included Facebook groups associated with different cities and regions in Germany, but also Facebook interest groups related to weather warnings, so as to include people who may have an interest in the survey topic and thus increase the number of potential participants. A total of 459 participants took part in the survey, of which we excluded three respondents due to a high amount of missing data. The remaining 456 participants (178 females, 271 males, and 7 unspecified) ranged in age from 15 to 66, with a mean age of 33.46.

4.3. Instrument validation

We validated our instruments through a confirmatory factor analysis (CFA) estimated with AMOS 25. The fit indices of this CFA indicate a good model fit (see [23]): $\chi^2(104) = 206.491$, TLI = 0.984, CFI = 0.989, NFI = 0.978, RFI = 0.968, IFI = 0.989, RMSEA = 0.047.

Table 2 illustrates the convergent validity of the constructs. The factor loadings of all items were highly significant ($p < 0.001$) and larger than 0.70. Also, Cronbach's Alpha of all constructs exceeded 0.90. Finally, the construct reliabilities were larger than the 0.6 benchmark [5], and the average variance extracted (AVEs) of all latent constructs was larger than 0.5 [14].

Table 2. Convergent validity

Con-struct	Indi-cator name	Factor loa-ding	Cron-bach's alpha	Comp. relia-bility	AVE
Risk Per-cep-tion	RP_3 RP_2 RP_1	0.933 0.915 0.927	0.947	0.947	0.856

Trust	Tr_3 Tr_2 Tr_1	0.821 0.95 0.861	0.907	0.910	0.772
Sub-jective Norm	SN_3 SN_2 SN_1	0.922 0.847 0.915	0.918	0.924	0.802
Data Se-curity	DS_3 DS_2 DS_1	0.959 0.986 0.916	0.968	0.968	0.910
Comp-liance Inten-tion	CI_1 CI_2	0.956 0.973	0.964	0.964	0.930
Usage Inten-tion	UI_1 UI_2 UI_3	0.963 0.971 0.971	0.978	0.978	0.938

With respect to discriminant validity, the correlation of each latent construct with all other constructs (see Table 3) was lower than the square root of the AVE for each construct [14]. Thus, evidence for discriminant validity is provided.

Table 3. Correlations and AVEs

Construct	1	2	3	4	5	6
1. Risk Perception	*.925*					
2. Trust	.376	*.879*				
3. Sub-jective Norm	.490	.529	*.895*			
4. Data Security	-.306	-.399	-.445	*.954*		
5. Compli-ance Intention	.512	.614	.649	-.495	*.965*	
6. Usage Intention	.542	.513	.684	-.610	.690	*.968*
The diagonal (italicized) represents the square root of the AVE scores.						

Since the psychometric properties of the scales are good, we proceed to the estimation results of the structural model.

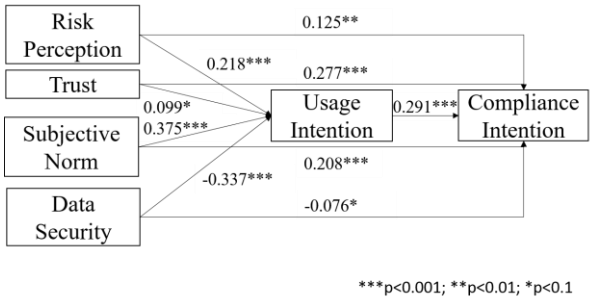
5. Results

Table A1 in the Appendix illustrates the estimation results of the structural equation model with full information maximum likelihood estimation. The model explains 63.1 percent of the variance of usage intention and 60.7 percent of the variance of compliance intention. Fit indices were all good: $\chi^2(104) = 206.491$, TLI = 0.984, CFI = 0.989, NFI = 0.978, RFI = 0.968, IFI = 0.989, RMSEA = 0.047.

H1a predicted a positive effect of risk perception on warning app usage intention, and is strongly supported (coefficient = 0.218, $p < 0.001$). Also, H1b, which predicted a positive effect of risk perception on intention to comply immediately, is supported (coefficient = 0.125, $p < 0.01$). Trust was hypothesized to have positive effects on warning app usage intention (H2a) and compliance intention (H2b). The path coefficients are significant (coefficients = 0.099 / 0.277, $p < 0.05$ / 0.001), and thus support both hypotheses. H3a/b examined the effects from subjective norm on warning app usage intention as well as compliance intention. Again, both effects were found to be highly statistically significant in support of H3a/b (coefficients = 0.375 / 0.208, $p < 0.001$). The only hypotheses that predicted negative effects of the independent variables on warning app usage intention and compliance intention were the hypotheses that included data security (H4a/H4b). Both hypotheses were supported (coefficients = -0.337 / -0.076, $p < 0.001$ / 0.1). Finally, H5 (warning app usage intention positively affects compliance intention) was also supported (coefficient = 0.291, $p < 0.001$).

Figure 2 is an overview of our results.

Figure 2. Research model validation using data from survey



We proceed with a discussion of our results in the next section.

6. Discussion

6.1. Implications for IS research

Prior research in the field of warning technology has focused on identifying the antecedents of students' intention to use warning systems or comply with warning messages, but has left intention to use warning systems among the public to future research [20]. Thus, our findings add to research on technology usage of the public in the context of emergency notifications and crisis warning.

As expected, the perceived probability of being directly affected by a crisis shows a positive correlation

with the intention to use mobile warning apps and the intention to comply with recommendations for action, which is in accordance to [20]. However, this stands in contradiction to previous findings in IS security research, which did not find support for a positive effect of risk perceptions (i.e., perceived severity) on behavioral compliance intentions with information systems' security policies [24]. One explanation could be that the threat in IS security research concerns data or information security and is not a personal threat such as a crisis event.

Also, perceived trust influences both the intention to use the app as well as the intention to comply with recommendations for action. Hence, if people perceive that they will receive relevant, accurate, and timely warnings, they are more likely to use a warning app and comply with the information received. The latter result is also consistent with prior findings of [20], who identified trust as an important factor to comply with campus emergencies.

Our findings further indicate that people's intention to use a warning app is affected by important others. If an individual cares more about the expectations of other people, that person is more likely to use a warning app and comply with the recommendations for action. This finding is also in accordance with prior research in the context of campus emergencies that investigated the usage intention of warning systems [2].

In addition, concerns about data security have a strong negative impact on the use of a warning app and a weak negative effect on compliance intention. Thus, our finding adds to research in risk communication and technology usage in the warning context by indicating that data security is an important factor when people decide to use a warning system.

Furthermore, people's motivation to comply with recommendations for action stems not only from their perception with respect to risk, trust, subjective norm, and data security, but also their warning app usage intention. In particular, we found that the intention to use a warning app positively influences people's compliance intention, which indicates that people who intend to use a warning app are also likely to carry out the recommended behavior suggested via the app.

Finally, our posited predictors explain 63.1 percent of the variance of usage intention and 60.7 percent of the variance of compliance intention, suggesting that the UTAUT and the findings of research on campus emergencies serve as a useful theoretical foundation in the warning app usage context.

6.2. Implications for practice

Major crisis events and minor threats such as street flooding or a thunderstorm can all injure or even kill people in an affected area. So, providers seeking to promote mobile warning app usage can point to both the likelihood of crises or threat situations, since people prepare only for threats they perceive as imminent [20], as well as explaining why warning apps are an effective means for receiving warning notifications. Pointing out the risk of such threats and that warning apps could help in warning people quickly and reliably would positively influence the use of warning apps.

We found that trust is an important influencing factor, too. Hence, to increase trust in their applications, providers should ensure the timeliness and correctness of their warnings. It is also important to explain why location-based settings are important for effective warnings and thoroughly explain the details of the providers' data security policies to decrease user concerns about data security that could hinder usage intention of warning apps.

Finally, subjective norm was found to be an important determinant of respondents' intention to use a warning app as well as to comply with situation-specific recommendations for action. Hence, to foster adoption of warning apps, providers could also incorporate mechanisms such as "recommend this app to a friend" into their warning apps.

6.3. Limitations and future research

Although the data generally supported the proposed model, there are some characteristics of our study that may limit generalizing our results. First, the participants were recruited from Facebook groups based in Germany. Thus, our sample comprised a subpopulation of potential smartphone users who also use social media. Second, since we also posted the questionnaire to Facebook interest groups related to weather warnings, our data collection also had a potential for self-selection bias, since participants recruited from such groups could be predisposed to obtaining weather warnings. Hence, further research using our method should be conducted among a different sample.

Furthermore, this study was conducted in Germany; therefore, care must be taken when generalizing these findings to users in other social and cultural environments. Future research should attempt to replicate this study in other countries. In particular, factors like data protection and security or risk perception could be perceived very differently in other countries.

As we are interested in the general use of warning apps, not their specific use during a crisis event, we opted not to take a scenario-based approach for collecting data. We measure people's general risk perception and thus our research focus on the usage of such apps beyond a specific crisis event. Prior research

on people's response to crisis events [21], however, also indicates that there are crisis-specific factors, which are important for analyzing people's protective behavior. For instance, the type of crisis is important for people to base their risk assessment and thus to perceive a certain amount of risk [21]. Additionally, in uncertain crisis situations people's decision on how to respond to a crisis depends on several factors, such as the interpretation of the warning message, the perceived relevance of the message, or the perception and recommendations of others [10]. Also, a person's stress level related to the crisis situation might influence usage intention and compliance intention. However, since crisis events occur infrequently and unpredictably and data collection during such events is ethically questionable behavioral observations are rather difficult. Hence, future research could analyze usage and compliance intention in different crisis settings, for instance, in a scenario-based research design.

Also, sex, race, and socio-economic status have been found to influence people's protective behavior [21]. [12], for example, analyzed the response of Hurricane Katrina survivors and conclude that strong racial and class difference influenced people's response to that crisis. Thus, future research could include control variables to analyze differences in protective behavior.

Finally, research indicates that a person's crisis experience is an important factor influencing people's protection behavior [18, 39], because people with personal crisis experience might see themselves as potential victim and perceive crisis as happening more frequently. Hence, future research could include experience with a crisis as further variable.

7. Conclusion

In this study, we investigated people's usage intention of a warning app and the intention to comply with recommendations for action transmitted via the app. We found that perceived risk, trust, and subjective norm have a positive effect on both variables. In addition, data security issues have a negative effect on usage and compliance intention.

Although a warning app alone does not ensure that people behave correctly in the event of a crisis or that all those affected will be warned, these apps have the potential to reach many people in a timely manner and transmit recommendations for action even before a crisis occurs. The more those affected are warned of a potential threat and the more they act in accordance with recommendations for action, the less there would be negative consequences of such an event.

Finally, not only warning apps but, of course, a variety of warning systems and communication channels should be used to ensure that people at risk receive warnings about crises, whether indoors or outdoors, at school, at home, or at work. Using the groundwork established in this study, future research in various possible directions could contribute to extending our theoretical understanding and practical ability to foster technology for public warnings.

References

[1] Ada, S., H.R. Rao, and R. Sharman, "Online social networking sites (SNS) use at the Campus emergencies", in Proceedings of the 31st International Conference on Information Systems. 2010.

[2] Ada, S., R. Sharman, W. Han, and J.A. Brennan, "Factors impacting the intention to use emergency notification services in Campus emergencies: An empirical investigation", IEEE Transactions on Professional Communication, 59(2), 2016, pp. 89–109.

[3] Ajzen, I., "The theory of planned behavior", Organizational Behavior and Human Decision Processes, 50(2), 1991, pp. 179–211.

[4] Anderson, C.L. and R. Agarwal, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions", MIS Quarterly, 34(3), 2010, pp. 613–643.

[5] Bagozzi, R.P. and Y. Yi, "On the evaluation of structural equation models", Journal of the Academy of Marketing Science, 16(1), 1988, pp. 74–94.

[6] Bamberg, S., I. Ajzen, and P. Schmidt, "Choice of travel mode in the theory of planned behavior: The roles of past behavior, habit, and reasoned action", Basic and Applied Social Psychology, 25(3), 2003, pp. 175–187.

[7] Boss, S.R., D.F. Galletta, P.B. Lowry, G.D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", MIS Quarterly, 39(4), 2015, pp. 837–864.

[8] Botterell, A. and R. Addams-Moring, "Public warning in the networked age: Open standards to the rescue?", Communications of the ACM, 50(3), 2007, pp. 59–60.

[9] Bubeck, P., W.J.W. Botzen, and J.C.J.H. Aerts, "A review of risk perceptions and other factors that influence flood mitigation behavior", Risk Analysis: An Official Publication of the Society for Risk Analysis, 32(9), 2012, pp. 1481–1495.

[10] Dash, N. and H. Gladwin, "Evacuation decision making and behavioral responses: Individual and

household", Natural Hazards Review, 8(3), 2007, pp. 69–77.

[11] Davis, F.D., "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, 13(3), 1989, pp. 319–340.

[12] Elliott, J.R. and J. Pais, "Race, class, and Hurricane Katrina: Social differences in human responses to disaster", Social Science Research, 35(2), 2006, pp. 295–321.

[13] Fischer, D., O. Posegga, and K. Fischbach, "Communication barriers in crisis management: A literature review", in Proceedings of the European Conference on Information Systems. 2016.

[14] Fornell, C. and D.F. Larcker, "Evaluating structural equation models with unobservable and measurement error", Journal of Marketing Research, 18(1), 1987, pp. 39–50.

[15] Franko, O.I. and T.F. Tirrell, "Smartphone app use among medical providers in ACGME training programs", Journal of medical systems, 36(5), 2012, pp. 3135–3139.

[16] Freberg, K., "Intention to comply with crisis messages communicated via social media", Public Relations Review, 38(3), 2012, pp. 416–421.

[17] Glik, D.C., "Risk communication for public health emergencies", Annual Review of Public Health, 28, 2007, pp. 33–54.

[18] Grothmann, T. and F. Reusswig, "People at risk of flooding: Why some residents take precautionary action while others do not", Natural Hazards, 38(1-2), 2006, pp. 101–120.

[19] Han, W., S. Ada, R. Sharman, R.H. Gray, and A. Simha, "Factors impacting the adoption of social network sites for emergency notification purposes in universities", International Journal of Business Information Systems, 18(1), 2015, pp. 85–106.

[20] Han, W., S. Ada, R. Sharman, and H.R. Rao, "Campus emergency notification systems: An examination of factors affecting compliance with alerts", MIS Quarterly, 39(4), 2015, pp. 909–929.

[21] Helsloot, I. and A. Ruitenberg, "Citizen response to disasters: A survey of literature and some practical implications", Journal of Contingencies and Crisis Management, 12(3), 2004, pp. 98–111.

[22] Herath, T. and H.R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations", European Journal of Information Systems, 18(2), 2009, pp. 106–125.

[23] Hu, L.-t. and P.M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1999, pp. 1–55.

[24] Ifinedo, P., "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", Computers & Security, 31(1), 2012, pp. 83–95.

[25] Johnston, A.C. and M. Warkentin, "Fear appeals and information security behavior: An empirical study", MIS Quarterly, 34(3), 2010, pp. 549–566.

[26] Johnston, A.C., M. Warkentin, and M. Siponen, "An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric", MIS Quarterly, 39(1), 2015, pp. 113–134.

[27] https://katwarn.de, accessed 12-29-2017.

[28] Leaning, J. and D. Guha-Sapir, "Natural disasters, armed conflict, and public health", The New England Journal of Medicine, 369(19), 2013, pp. 1836–1842.

[29] Lee, D., J.Y. Chung, and H. Kim, "Text me when it becomes dangerous: Exploring the determinants of college students' adoption of mobile-based text alerts short message service", Computers in Human Behavior, 29(3), 2013, pp. 563–569.

[30] Lee, Y. and K.R. Larsen, "Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software", European Journal of Information Systems, 18(2), 2009, pp. 177–187.

[31] Mayhorn, C.B., M. Yim, and J.A. Orrock, "Warnings and hazard communication for natural and technological disasters", in Handbook of Warnings, M.S. Wogalter, Editor. 2006. Lawrence Erlbaum Associates, Publishers: Mahwah, New Jersey, London.

[32] Meissen, U., M. Hardt, and A. Voisard, "Towards a general system design for community-centered crisis and emergency warning systems", in Proceedings of the 11th International Conference on Information Systems for Crisis Response. 2014.

[33] Milne, S., S. Orbell, and P. Sheeran, "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions", British Journal of Health Psychology, 7(May), 2002, pp. 163–184.

[34] Mousavizadeh, M. and D.J. Kim, "A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of

protection motivation theory", in Proceedings of the 36th International Conference on Information Systems. 2015.

[35] Pew Research Center, "Smartphone ownership and internet usage continues to climb in emerging economies. But advanced economies still have higher rates of technology use", 2016.

[36] Reuter, C., M. Kaufhold, I. Leopold, and H. Knipp, "KATWARN, NINA, or FEMA? Multi-method study on distribution, use, and public views on crisis apps", in Proceedings of the 25th European Conference on Information Systems. 2017.

[37] Slovic, P., B. Fischhoff, and S. Lichtenstein, "Rating the risk", in Readings in Risk, T.S. Glickman and M. Gough, Editors. 1990. Resour. Fut: Washington, DC.

[38] Solberg, C., T. Rossetto, and H. Joffe, "The social psychology of seismic hazard adjustment: Re-evaluating the international literature", Natural Hazards and Earth System Science, 10(8), 2010, pp. 1663–1677.

[39] Thieken, A.H., H. Kreibich, M. Müller, and B. Merz, "Coping with floods: Preparedness, response and recovery of flood-affected residents in Germany in 2002", Hydrological Sciences Journal, 52(5), 2007, pp. 1016–1037.

[40] Tversky, A. and D. Kahneman, "Rational choice and the framing of decisions", The Journal of Business, 59(4), 1986, pp. 251–278.

[41] Venkatesh, V., M.G. Morris, G.B. Davis, and F.D. Davis, "User acceptance of information technology: Toward a unified view", MIS Quarterly, 27(3), 2003, pp. 425–478.

[42] Venkatesh, V., J.Y.L. Thong, and X. Xu, "Unified theory of acceptance and use of technology: A synthesis and the road ahead", Journal of the Association for Information Systems, 17(5), 2016, pp. 328–376.

[43] Voss, M. and K. Wagner, "Learning from (small) disasters", Natural Hazards, 55(3), 2010, pp. 657–669.

[44] http://www.bbk.bund.de/DE/NINA/Warn-App_NINA.html, accessed 12-29-2017.

[45] Wogalter, M.S., "Purposes and scope of warnings", in Handbook of Warnings, M.S. Wogalter, Editor. 2006. Lawrence Erlbaum Associates, Publishers: Mahwah, New Jersey, London.

[46] Wogalter, M.S., M.J. Kalsher, and R. Rashid, "E!ect of signal word and source attribution on judgments of warning credibility and compliance likelihood", International Journal of Industrial Ergonomic, 24, 1999, pp. 185–192.

[47] Xu, H., H.-H. Teo, and B. Tan, "Predicting the adoption of location-based services: The role of trust and perceived privacy risk", in International Conference on Information Systems. 2005.

Appendix

Table A1. Model results

Structural Path			**Estimate**	**S.E.**	**Stand. Estimate**	**t**	**p**	**Hypo-thesis**	**Conclu-sion**
Usage Intention	<---	Risk Perc.	0.291	0.049	0.218	5.933	***	H1a	supported
Compliance Int.	<---	Risk Perc.	0.119	0.038	0.125	3.135	0.002	H1b	supported
Usage Intention	<---	Trust	0.147	0.058	0.099	2.545	0.011	H2a	supported
Compliance Int.	<---	Trust	0.294	0.044	0.277	6.656	***	H2b	supported
Usage Intention	<---	Subj. Norm	0.546	0.062	0.375	8.745	***	H3a	supported
Compliance Int.	<---	Subj. Norm	0.217	0.051	0.208	4.238	***	H3b	supported
Usage Intention	<---	Data Security	-0.361	0.038	-0.337	-9.539	***	H4a	supported
Compliance Int.	<---	Data Security	-0.058	0.031	-0.076	-1.88	0.06	H4b	supported
Compliance Int.	<---	Usage Int.	0.208	0.039	0.291	5.4	***	H5	supported